IMPLEMENTASI KRIPTOSYSTEM MENGGUNAKAN METODE ALGORITMA ECC DENGAN FUNGSI MD5 PADA SISTEM DATABASE TICKETING ONLINE

IMPLEMENTATION OF CRYPTHOSYSTEM USING ECC ALGORITHM WITH MD5 FUNCTION IN ONLINE TICKETING SYSTEM DATABASE

Jaya Santoso Sirait[1] , R Rumani M [2] , Marisa W. Paryasto[3]

[1,2,3]Prodi S1 Sistem Komputer, Fakultas Teknik Elektro, Telkom University

Bandung, Indonesia

[1]jayasantososirait@gmail.com, [2]rumani@telkomuniversity.ac.id, [3]marisa.paryasto@telkomuniversity.ac.id

Keamanan data merupakan sesuatu yang penting di dalam perkembangan teknologi terutama di bidang teknologi informasi. Data yang tersimpan harus dapat terjamin keamanannya sehinga tidak menimbulkan penyalahgunaan data. Salah satunya dalam pembelian tiket, semakin berkembangnya zaman kita dapat membeli tiket secara online. Namum rentan akan pembobolan data terutama pada bagian data pembeli. Ada pun solusi untuk mengatasi pembobolan data tersebut sistem seharusnya memakai kriptografi. Dengan kriptografi pembeli dapat mengirimkan data secara aman, karena menggunakan proses enkripsi.

Dalam penelitian tugas akhir ini akan merancang suatu sistem yang dapat menjaga keamanan pada sistem pembelian tiket online dengan menggunakan Algoritma Kurva Eliptik dan MD5 dimana enkripsi dilakukan dengan public key dan verifikasi dengan fungsi MD5. Dari percobaan serangan dengan *Man in middle* tidak bisa terjadi karena tidak mempunyai publik key yang berbeda dengan server aslinya. Penggunaan algoritma ECC dan MD5 sangat di anjurkan untuk penggunaan suatu aplikasi terutama yang membutuhkan jaringan yang rentan akan serangan dan pencurian dari pihak lain.

Keyword : *Elliptic Curve Cryptosystem, Security* MD5, *securitysystem, encryption, decryption. database security*

Abstract

Data security is something that is important in the development of technology, especially in the field of information technology. The stored data must be secure so it does not cause data misuse. One of them in purchasing tickets, the growing times we can buy tickets online. However vulnerable to breaking data, especially on the data of buyers. There is also a solution to solve the data breaking system should use cryptography. With cryptographic buyers can transmit data securely, because it uses the encryption process.

In this final project will design a system that can maintain security on online ticket purchasing system by using Eliptic Curve Algorithm and MD5 where encryption is done with public key and verification with MD5 function. From the attack experiment with Man in middle can not happen because it does not have a different public key with the original server. The use of ECC and MD5 algorithms is strongly recommended for the use of an application especially requiring networks that are vulnerable to attack and theft from others.

Keyword : *Elliptic Curve Cryptosystem, Security* MD5, *securitysystem, encryption, decryption. database security*

1. Pendahuluan

Aplikasi dengan pemanfaatan teknologi jaringan komputer dan telekomunikasi berkembang dengan sangat pesat , banyak kegiatan manusia kini di bantu dengan teknologi tersebut , untuk melakukan pertukarn berbagi informasi .Dalam pertukaran infrormasi tersebut terdapat data data yang penting , misalnya dalam pembelian tiket transportasi secara online siapa saja bisa membeli dengan mudah.Dengan menggunakan sistem pembelian tiket secara online ,bisa terjadi pengambilan data data yang penting , maka kita membutuhkan suatu keamanan agar tidak terjadi pengambilan data yang tidak diinginkan.

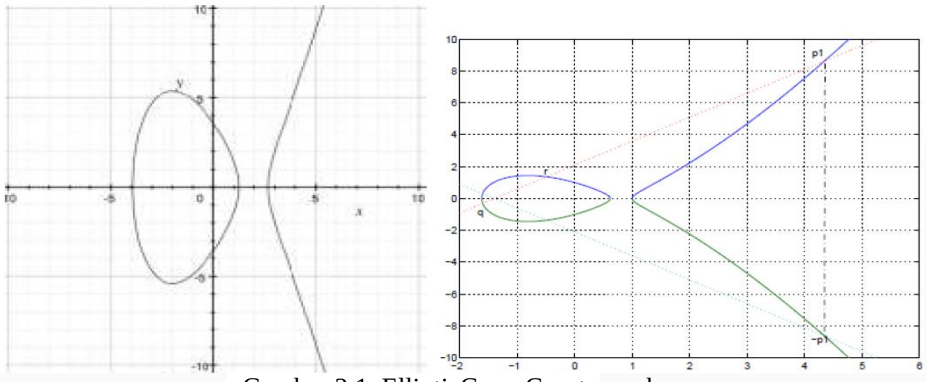
Kriptografi (*cryptography*) berasaldari Bahasa Yunani: "*cryptos*" artinya "*secret*" (rahasia), sedangkan "*graphein*" artinya "*writing*" (tulisan). Jadi kriptog rafiberarti "*secret writing*" (tulisanrahasia). Jadi dapat disimpulkan Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, sertaotentikasi [9].

MD5 adalah fungsi hash kriptografi yang digunakan secara luas dengan value 128-bit . pada standart internet , MD5 telah dimanfaatkan di berbagai macam aplikasi keamana , dan MD5 juga digunakan untuk melakukan pengujian integritas sebuah berkas [6].

2. Dasar Teori

2.1. Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC)termasuk sistem kriptografi kunci publik yang mendasarkan keamanannya pada permasalahan matematis kurva eliptik. Karena alasan tersebut, algoritma kriptografi kurva eliptik mempunyai keuntungan jika dibandingkan dengan algoritma kriptografi kuncipublik lainnya yaitu dalam hal ukuran panjang kunci yang lebih pendek tetapi memiliki tingkat keamanan yang sama. Penggunaan kurva elliptic dicetuskan oleh Neal Koblitzdan Victor S. Miller padatahun 1985. [12]



Gambar 2.1. EllipticCurveCryptography

Adapun untuk membuat EllipticCurveCryptosystem diperlukan penjumlahan dua titik pada kurva Elips E(Fp) yang menghasilkan titik ke tiga pada kurva elips. Aturan ini dapat dijelaskan secara geometris sebagai berikut.

$$y^2 = x^3 + ax + b + \text{c dengan} 4a^3 + 27b^2 \neq 0 \quad (1)$$

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \\ \frac{3{x_1}^2 + a}{2y_1} \end{cases} \quad (2)$$

Diberikan E olehy$^2 = x^3 + bx + c$ dan P1 = (x_1, y_1) dan P2 = (x_2, y_2)P1 + P2 = P3 (x_3, y_3)

Maka diperoleh (x3, y3) sebagai berikut :

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda(x_1 + x_3) - y_1 \quad (3)$$

Pada operasi perkalian titik, titik P pada kurva eliptik dikalikan dengan k (bilangan scalar) dengan menggunakan persamaan tersebut untuk mendapatkan titik Q padakurva yang sama, maka

$$kP = Q$$

adapun operasi perkaliannya ialah sebagai berikut.

a. Operasi pertambahan titik, yaitu menambahkan dua buah titik J dan K untuk mendapatkan titik L. Dengan demikian L = 2J.

b. Operasi penggandaan titik, yaitu menambahkan titik J dengan dirinya sendiri untuk mendapatkan titik L. Dengan demikian L = 2J.

Operasi penjumlahan pada *elliptic curves* disebut tangent and chord method. Operasi tersebut dapat dijabarkan sebagai berikut misalkan $(x_1 - y_1)$, $(x_2 - y_2)$, dan $(x_3 - y_3)$ melambangkan koordinat, P, Q dan $P + Q$. $(x_3 - y_3)$ dinotasikan dalam x_1, y_1, x_2, y_2 . Didefinisikan $P + Q$, misalkan $y = \propto x + \beta$ merupakan persamaan garis yang melalui P dan Q dan bukan merupakan garis vertikal pada kasus 3, maka didapatkan $\propto = (y_2 - y_1) / (x_2 - x_1)$ dan $\beta = y_1 - \propto x_1$. Suatu titik pada l, yaitu $(x, \propto x + \beta)$ terletak pada kurva jika dan hanya jika $(x, \propto x + \beta)^2 = x^3 + ax + b$, maka hanya akan terdapat satu titik potong untuk setiap akar persamaan kubik $x^3 + (\propto x + \beta)^2 + ax + b$. Telah diketahui terdapat dua akar yaitu $x_1$dan x_2, Karena $(x_1, \propto x_1 + \beta)$ dan $(x_2 \propto x_2 + \beta)$ merupakan titik P dan Q. Karena jumlah dari akar polynomial monik sama dengan negatif koefisien dari pangkat kedua tertinggi, maka dapat disimpulkan $x_3 = \propto^2 - x_1$.Sehingga didapat persamaan, P + Q = (x3, – (∝x3 + β) yang jika dinotasikan dalam x1, y1, x2, y2 sebagai berikut.

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2;$$

$$y_3 = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - (x_1 - x_3)^2 \qquad (10)$$

Pada kasus 5) dimana P = Q, persamaan yang didapatkan hampir mirip hanya saja ∞ diganti dengan turunan $\frac{dy}{dx}$di P. Turunan dari persamaan $y^2 = x^3 + ax + b$ di dapat dari formula $\alpha = \left(\frac{3x_1^2 - a}{2y_1}\right)$. Perhitungannya adalah sebagi berikut.

$$y^2 = x^3 + ax + b$$

$$2y\frac{dy}{dx} = 3x^2\frac{dy}{dx} + a\frac{dy}{dx} + 0$$

Dari perhitungan di atas didapatkan dari nilai α sehingga formula untuk mencari nilai 2p adalah sebagai berikut.

$$x_3 = \left(\frac{3x^2 - a}{2y}\right)^2 - x_1 - x_2;$$

$$y_3 = -y_1 + \left(\frac{3x^2 - a}{2y}\right)^{2\,2} - (x_1 - x_3) \qquad (11)$$

Contoh perhitungan untuk memperjelas ilutrasi di atas adalah sebagai berikut:
Misalkan pada persamaan *eliptic curves* $y^2 = x^3 - 36x, P = (-3,9) dan\ Q = (-2,8)$ merupakan titik-titik dimana yang terdapat dalam persamaan tersebut.Akan dicari P+Q dan 2P, proses yang dilakukan.

a) P+ Q

Subtitusikan $x_1 = -3, y_1 = 9, x_2 = -2, y_2 = 8$.pada persamaan (10) menghasilakn $x_3 = 6$,sedankan persamaan kedua di dapat $y_3 = 0$

$$x_3 = \left(\frac{8 - 9}{-2 - (-3)}\right)^2 (-3 - 6)$$

$x_3 = 6;$

$$y_3 = -9 + \left(\frac{8 - 9}{-2 - (-3)}\right)^2 (-3 - 6)$$

$$y_3 = 0$$

Jadi nilai P + Q = (6,0).

b) 2P

Subtitusikan $x_1 = -3, y_1 = 9, a = -36$ .pada persamaan (11) yang menghasilkan $x_3 = \frac{15}{4}\ dan\ y_3 = \frac{-35}{8}$

$$x_3 = \left(\frac{3(-3)^2 - (-36)}{2(9)}\right)^2 - 2(-3);$$

$$x_3 = \frac{25}{4}$$

$$y_3 = \left(\frac{3(-3)^2 - (-36)}{2(9)}\right)^2 (-3 - \frac{25}{4})$$

$$y_3 = \frac{-35}{8}$$

Jadi di dapatkan nilai $2P = (\frac{25}{4}, \frac{-35}{8})$

Perkalian dalam *eliptic curves* dinotasikan sebagai nP, yang didefinisikan sama seperti group abelian lain, yaitu menambahkan P sebanyak n kali pada titik itu sendiri jika n positif atau menambahkan –p pada dirinya sendiri sebanyak |n| kali jika n negatif [3].

2.2. MD5

MD5 adalah fungsi hash satu arah yang dibuat oleh Ronal Rivest pada tahun 1991.MD5 merupakan perbaikan dari MD4 setelah MD4 berhasil di serang oleh kriptanalis .Algoritma message digest yang panjangnya 128 bit. Langkah–langkah pembuatan *message* digest secara garis besar adalah sebati berikut.

a. Penambahan bit-bit pengganjal (*padding bits).*

Pesan ditambahkan dengan sejumlah bit pengganjal sedimkian sehingga panjang pesan (dalam satuan bit) kongruen dengan 448 modulo 512. Ini berarti panjang pesan setelah ditambahi bit-bit pengganjal adalah 64 bit kurang dari kelipatan 512.Angka 512 ini muncul karena MD5 memproses pesan dalam blok-blok yang berukuran 512. Pesan dengan panjang 448 bit pun tetap ditambah dengan bit-bit pengganjal. Jika panjang pesan 448 bit, maka pesan tersebut di tambah dengan 512 bit menjadi 960 bit. Jadi, panjang bit-bit pengganjal adalah anatara 1 sampai 512. Bit-bit pengganjal terdiri dari sebuah bit 1 diikuti dengan sisanya bit 0.

b. Penambahan nilai panjaang pesan semula.

Pesan yang telah diberi bit-bit pengganjal selanjutnya ditambah lagi dengan 64 bit yang menyatakan panjang pesan semula. Jika panjang pesan $>2^{64}$ maka yang diambil adalah panjangnya dalam modulo 2^{64} .Dengan kata lain, jika panjang pesan semula adalah K bit, maka 64 bit yang ditambahkan menyatakan K modulo 2^{64} . Setelah ditambahkan dengan 64 bit, panjang pesan sekarang menjadi kelipatan 512 bit.

c. Inisialisasi penyangga (*buffer)* MD.

MD5 membutuhkan 4 buah penyangga (*buffer)* yang masing masing panjangnya 32 bit. Total panjang penyangga adalah 4 x 32 = 128 bit. Keempat penyangga ini menampung hasil antara dan hasil akhir. Keempat penyangga ini diberikan nama A, B, C, dan D. Setiap penyangga diinisialisasi dengan nilai (dalam notasi HEX) sebai berikut.

A = 01234567

B = 89ABCDEF

C = FEDCBA98

D = 76543210

(Catatan : beberapa versi MD5 menggunakan nilai inisialisasi berbeda, yaitu.

A = 67452301

B = EFCDAB89

C = 98BADCFE

D = 10325467)

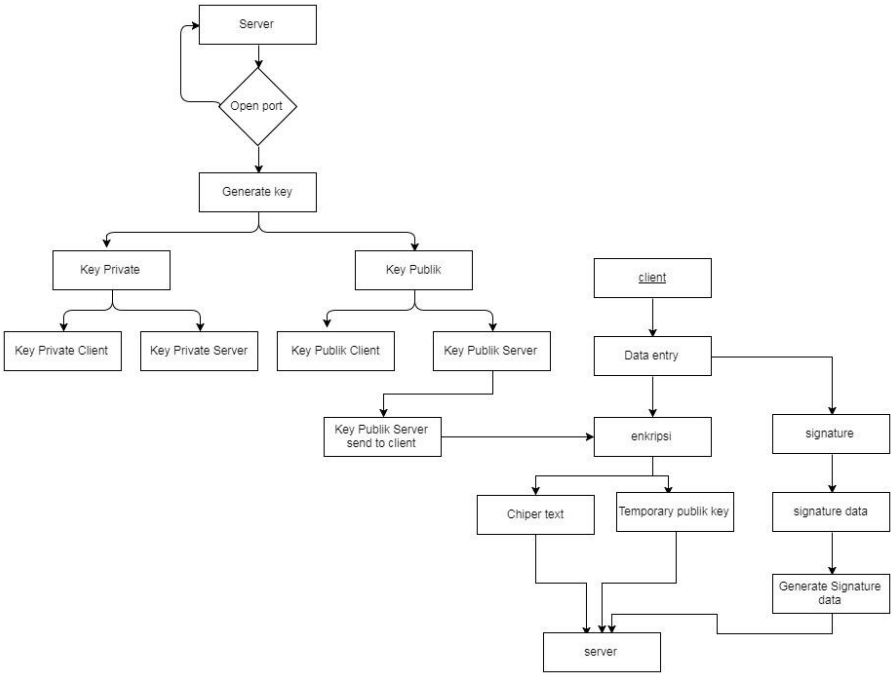
d. Pengolahan pesan dalam blik berukuran 512 bit.

Pesan dibagi menjadi *L* buah block yang masing-masing panjangnya 512 bit (Y_0 sampai Y_{L-1}). Setiap block 512-bit diproses bersaaab debgab penyangga MD mejadi keluaran 128-bit, dan ini disebut proses H_{MD5}.Proses H_{MD5} terdiri dari 4 buah putaran, dan masing-masing putaran melakukan operasi dasar MD5 sebanyak 16 kali dan setiap operasi dasar memakai sebuah elemen T [9].

3. Pembahasan

3.1. Deskripsi Sistem

Algoritma ECC sebagaisertifikat digital (*Digital Certificate)* untuk membuat suatu system itu dipercaya oleh user ketika melakukan transaksi di aplikasi tersebut. Sedangkan MD5 sebagai tanda tangan digital (*Digital Signature*) yang berfungsi sebagai penvalidasi bahwa data yang diterimaoleh server tersebut asli berasal dari user. Dan pada user diberikannya ECC dan MD5 pada program tersebut sehingga data yang telah di enkripsi dapat langsung di dekripsi oleh server untuk mengecek keaslian data tersebut.

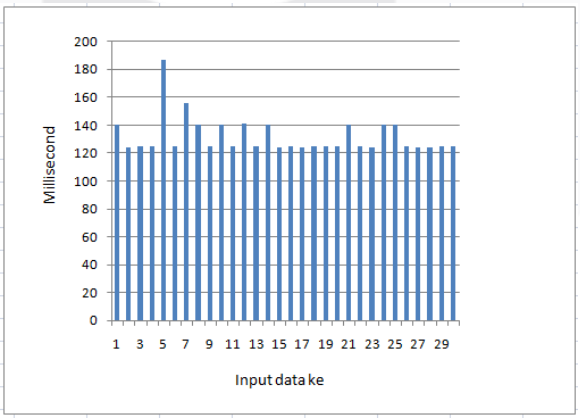


Gambar 3.1. Flowchart Skema Sistem

*3.2.*Pengujian dan Analisa

3.2.1. Pengujian Time Response

Time Response adalah waktu yang dibutuhkan ketika client mengirimkan permintaan data ke server dan pertukaran kunci yang dilakukan oleh kedua pihak. Pada tugas akhir ini pengukuran Time Response dimulai dari keadaan data yang telah di submit yang memiliki panjang kunci dan dengan waktu yang dibutuhkan.



Gambar 3.2. Diagram Time Response

Gambar diatas menunjukkan bahwa jumlah penginputan data yang dilakukan sebanyak 30kali dengan menggunakan kunci ECC dan MD5. Dengan timerespond rata-rata 131.93 milisecond.

3.3. Analisa Tingkat Keamanan.

Setelah melakukan pengujian dengan time respond perbandingan dengan SHA-256, tidak luputnya kita mendapatkan analisa dari berbagai jenis serangan yang dapat dilakukan terhadap aplikasi yang dibuat. Adapun jenis-jenis serangan yang dapat dilakukan ialah Spoofing, Sniffing, dan Man in Middle Attack.

3.3.1. Spoofing

Seperti yang kitaketahui Spoofing ialah jenis serangan yang dilakukan oleh attacker atau seseorang yang tidak bertanggung jawab untuk mencoba menelusuri atau menyeludup sebuah jaringan dengan mengirimkan pemberitahuan bahwa paket ini sangat dipercaya untuk melakukan hosting pengisian data dll. Untuk menghindari serangan spoofing ini kita melakukan dengan pembuatan filter yang berfungsi untuk menghadang siattacker untuk melakukan penelusupan dengan cara enkripsi.

3.3.2. Sniffiing

Adapun ancaman selanjutnya untuk client dan server ialah ada Serangan Sniffing. Serangan Sniffing ialah serangan yang bermaksud menyabotase atau mengambil alih data yang dimiliki kemudian mengubah datanya dan diteruskan kepada data tujuan. Adapun cara-caranya agar tidak terjadi kasus ini ialah dengan membuat server fake yang bertujuan untuk melindungi server yang aslinya.

3.3.3. Man in Middle Attack

Serangan yang terjadi pada tipe ini adalah adanya pencobaan pengambilan atau perubahan data pada saat terjadi pertukaran data antara client dengan server .Maka dengan adanya Proses Enkripsi dan pertukaran kunci ini. Diharapkan Attacker tidak dapat menyerang proses yang sedang terjadi. Dan apabila attacker tetap bersikukuh ingin menyerang dengan menyamar, Server tetap meminta permintaan Private key / MD5 yang dimana itu hanya dimiliki oleh Server Tersebut. Sehingga Attacker tidak dapat melakukan penyerangan.

4. Kesimpulan dan Saran

4.1. Kesimpulan

Setelah dilakukan beberapa pengujian dan analisa, dapat kita simpulkan beberapa hal yaitu.

1. Penggunaan Algoritma ECC dan MD5 untuk penggunaan suatu aplikasi yang memerlukan proses komputasi yang lebih cepat dari SHA-256.
2. Pengujian dan Analisis yang dilakukan ialah dengan menguji *Response Time* yang merupakan parameter keberhasikan dari pengujian sistem tersebut.
3. *Response Time* yang telah diujicoba oleh aplikasi dengan melalui Proses Enkripsi, Dekripsi dan Signature Data dengan rata-rata 131.93 ms dalam 30 kali percobaan.
4. Adapun jenis jenis serangan yang sudah dianalisa ialah Spoofing, Sniffing, dan Man in Middle. Spoofing dapat diatasi dengan penggunaan fungsi enkripsi dan dekripsi pada suatu proses.Aplikasi ini dapat mengelabui Sniffing dikarenakan memiliki Fake Server yang dimana sudah membuat fungsi ghost sebagai pelindung dari serangan dan Man In The Middle dapat diatasi dengan penggunaan MD5 Sebagai Signature Key dalam proses authentikasi data yang digunakan untuk memeriksa keaslian data tersebut.

4.2. Saran

Terlepas dari masih banyak kekurangannya Tugas Akhir ini. Penulis memiliki saran untuk penelitian selanjutnya:

1. Diharapkan pada penilitian selanjutnya, Dapat dikembangkan dari tidak hanya Client dan Server yang menggunakan 1 device. Tetapi bisa menggunakan berbagai device.
2. Dikembangkannya sistem login dan password. Saat ini belum bisa dikembangkan di karenakan masih terbatasnya kemampuan yang dimiliki.
3. Mampu menganalisa untuk berbagai macam kasus serangan yang lainnya.
4. Jenis pengujian aplikasi dapat lebih beragam.

DAFTAR PUSTAKA

[1] Andi Gutmans, Stig Seather B, Derick Rethans, "PHP5 Power Programming," Prentice Hall, pp. 111, 2005.

[2] Budi Raharjo, 2015 ,Mudah Belajar Python untuk Aplikasi Desktop dan Web, Bandung :Penerbit Informatika.

[3] Dinis sya'ban,2007 ,Elliptic Curves Crytograpy,Bogor :Sekolah Tinggi Sandi Negara.

[4] Fita PS,Irnawati, Rini H, Dewi Ekawati,S.km,Windiarto S.kom, 2013,Pembuatan Software Rekam medis Dengan Java NetBeans+MYSQL),Yogyakarta :Penerbit Gava Media.

[5] Herbert Schildt, "The Complete Reference, Seventh Edition (Osborne Complete Reference Series)," Java Programming, pp. 6-8, 2015.

[6] Inayatullah, 2007, Analisis Penerapan Algoritma MD5 Untuk Pengamanan Password . Palembang : STMIK MDP PALEMBANG.

[7] Komputer, Wahana., 2010, The Best Encryption Tools, Jakarta : Elex Media Komputindo.

[8] Mattes, Daniel., Starkey Chad, 2013, Verification of Online Transactions, California : Jumio Inc.,

[9] Munir, Rinaldi., 2006, Kriptografi, Bandung : Penerbit Informatika.

[10] Ponomarev, Oleg., Khurri, Andrey., Gurtov, Andrei, 2010, Elliptic Curve Cryptography (ECC) for Host Identity Protocol (HIP), Finland : Helnsinki Institute for Information Technology HIT/ Aalto University.

[11] Purbadian Y, "Aplikasi Penjualan Web Base Dengan PHP Untuk Panduan Skripsi," ASFA Solution, pp.2-24, 2015.

[12] Rodriguez-Henriquez, Fransisco., Saqib, N.A., **Koc**, Cetin Kaya., 2006, *Cryptographic Algorithms on Reconfigurable Hardware*, United Stated of America : Springer Science+Business Media, LLC.

[13] Warno ,"Pembelajaran Pemrograman Bahasa Java dan Arti Keyword," Jurnal Komputer, vol. 8, no. 1, pp. 40-51, 2012.

[14] Welling L, Thomson L, "PHP and MySQL Web Development, Fourth Edition," , Pearson Education, Inc, pp. 2, 2009.